AMR Cyber Security

DORA
WHITE PAPER

NOVEMBER 2024
VERSION: 1.0

PUBLIC RELEASE

TABLE OF CONTENTS

Document History

Version	Status	Date	Author
0.1	Issued	08/10/2024	Justin Greenwood-Delgado
0.2	QA Review	06/11/2024	Sean McCarthy
1.0	Final Release	08/11/2024	Martin Walsham

1.0 Introduction

AMR CyberSecurity is a CHECK, CREST and STAR approved company with a team of experienced principal consultants holding the highest technical qualifications. AMR CyberSecurity was founded with a clear mission: to provide exceptional human-led penetration testing and security assurance services, helping organisations we partner with effectively minimise their security risks.

AMR CyberSecurity works with you to protect your brand, your assets, and your reputation against the increasing real-world threat of cyber-attack and digital security compromise.

And now, AMR CyberSecurity's new DORA assurance and testing service is designed to assist organisations within the insurance and financial sector in adhering and maintaining compliance within this nascent European security framework.

1.1 What Is DORA

The Digital Operational Resilience Act (DORA) - Regulation (EU) 2022/2554, or DORA as it is known within the industry, is an EU financial regulation. That solves an important problem with operational risk; outlining governance rules for the protection, detection, containment, recovery and repair capabilities against ICT-related incidents.

It is a regulation that entered into force on 16 January 2023, but until recently has been on the back burner for most organisations due to compliance and enforcement not being **required** until **17 January 2025**.

This is an EU regulation — not a directive — and there is a difference between how EU directives and regulations impact member states.

The EU has two types of legal instruments:

- **Directives** set minimum standards and parameters for the EU but leave the actual implementation to member states themselves. When a directive is passed, the EU sets a deadline by which every member state must put the directive into force, whether by law, regulation or other initiative.

- **Regulations**, on the other hand, apply across the EU with the same authority as if they were local laws. Member states may choose to pass their own laws to implement a regulation (often because the regulation requires each state to define some detail individually), but the regulation will apply regardless.

1.2 Why DORA Is Needed

This Regulation acknowledges that ICT incidents and a lack of operational resilience have the possibility to jeopardise the soundness of the entire financial system, even if there is "adequate" capital for the traditional risk categories. Though bringing in formal regulation, it enforces a minimum standard and the knowledge that a level of risk is being managed and provisioned for. DORA has the additional benefit in outlining regulation in the following areas:

- Rules for an oversight framework for critical ICT third-party service providers when providing services to financial entities
- Rules on cooperation among supervisory authorities, and on supervision and enforcement
- Requirements in relation to contractual arrangements between financial entities and ICT third-party service providers.

DORA is managed by the three European supervisory authorities: the EBA (European Banking Authority), EIOPA (European Insurance and Occupational Pensions Authority) and ESMA (European Securities and Markets Authority).

For more information on the specifics of the Act please refer to the following EU managed website:

- https://www.digital-operational-resilience-act.com/

1.3 Who Does The DORA Regulation Apply To?

The DORA Regulation applies to the EU's insurance and financial sectors and any suppliers of ICT services to that sector, regardless of where those suppliers are based globally.

Financial entities covered by the Regulation include:

- Credit institutions
- Payment institutions
- Account information service providers
- Electronic money institutions
- Investment firms
- Central securities depositories
- Central counterparties
- Trading venues
- Trade repositories
- Managers of alternative investment funds
- Management companies
- Data reporting service providers
- Insurance and reinsurance undertakings
- Institutions for occupational retirement provision
- Credit rating agencies
- Administrators of critical benchmarks
- Crowdfunding service providers
- Securitisation repositories
- Crypto-asset service providers and issuers of asset-referenced tokens
- Insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries

The regulation mandates that these entities implement a comprehensive framework for digital operational resilience, covering risk management, incident reporting, testing, and oversight of third-party providers. By applying to such a wide spectrum of entities, DORA ensures a unified standard of resilience across the EU's financial ecosystem.

2.0 Specifics On Testing

In relation to security testing services, on 18 July, 2024, the European Supervisory Authorities (ESAs) published the final versions of their second batch of their draft regulatory technical standards (RTS) and implementing technical standards (ITS) developed under the Digital Operational Resilience Act (DORA), as well as two sets of Guidelines. The draft RTS for the delivery of DORA can be found here.
https://www.esma.europa.eu/sites/default/files/2024-07/JC_2024-29_-_Final_report_DORA_RTS_on_TLPT.pdf

The key takeaway from this is that it outlines DORA and the kinds of testing for 'Digital Operational Resilience Testing' under Chapter IV of the Final DORA text. The chapter contains 4 articles (24-27), which cover the general requirements, how to test ICT tools and systems, advanced testing of ICT tools and requirements for testers.

Article 25 prescribes the following tests for financial entities in the EU:

- Vulnerability assessments and scans
- Open-source analyses
- Network security assessments
- Gap analyses
- Physical security reviews
- Questionnaires and scanning software solutions
- Source code reviews (where feasible)
- Scenario testing
- Compatibility testing
- Performance testing
- End-to-end testing
- Penetration testing (aka, Threat-Led Penetration Testing or TLPT)

DORA necessitates that financial entities must conduct these resilience tests regularly. The frequency may vary based on the size, nature, and complexity of the organisation. The tests must also cover all critical ICT systems and tools, including those managed by third-party providers.

Article 26 of DORA goes deeper into its mandate for Threat Led Penetration Testing (TLPT).

Here's a brief look at what the advanced testing of ICT tools, systems and processes based on TLPT requires:

1. **Frequency:** Financial entities, other than microenterprises, must carry out advanced testing (TLPT) at least once every three years. The competent authority may increase or decrease this frequency based on the risk profile of the institution.

2. **Scope:** Each test must cover critical or important functions of the organisation, and the tests must be conducted on live production systems. Based on the institution's assessment of critical functions (including those outsourced to critical ICT third party service providers), the scope of the TLPT will be decided. This scope will then be validated by the competent authority.

3. **ICT Third Party Risk:** The onus of ensuring third party participation in the test (if they fall into the scope of the TLPT), lies with the financial institution.

4. **Pooled Testing:** EU DORA allows financial entities to conduct pooled threat-led penetration testing (TLPT) for third-party service providers. This means multiple financial entities can collaborate to test a shared ICT service provider's security. This pooled test can be performed by an external tester but under the direction of one designated financial entity.

2.1 What Is Threat-Led Penetration Testing?

Threat-Led Penetration Testing (TLPT) is an advanced cybersecurity assessment that involves intelligence-driven simulations of real-world cyberattacks on an organisation. Unlike traditional penetration testing, TLPT is conducted in secrecy with only key organisation heads being aware of the activity and with the organisation's defence team unaware that a test is taking place. This allows for full assessment of the effectiveness of deployed controls, responses and procedures to sophisticated attacks on the organisation, derived from the detailed threat intelligence and adversaries unique to the organisation.
A Red Team replicates the tactics of these specific threat actors, targeting a wide range of systems, processes, and personnel.

2.2 What's The Difference Between TLPT & TIBER?

The DORA regulation was largely modelled after the existing TIBER-EU framework. However, there are a few differences between their adoption when applied to DORA.

1. The regulators are defined more specifically in TIBER than in DORA. DORA gives Member States more freedom in this regard.

2. Internal testing is not allowed under TIBER, but is allowed under DORA - with a few conditions. Internal TLPT is only allowed two out of three times; the third time an outside party has to perform the TLPT. In all cases, the threat intelligence used for internal TLPT also has to be provided by an outside party.

3. Purple Teaming is strongly recommended by TIBER-EU, but is not compulsory. Under DORA purple teaming is compulsory. This means working together with and training the Blue Team, or a company's defenders, is integrated into the DORA regulation. Often, this is done at the end of the exercise.

3.0 Overview of Testing Organisations

AMR CyberSecurity has a proven track record and body of experience helping organisations from every sector meet their IT governance, risk management and compliance objectives. As outlined below, we are proud to hold all the key industry recognised certifications, promoting our capabilities in delivering the highest standard of certified services.

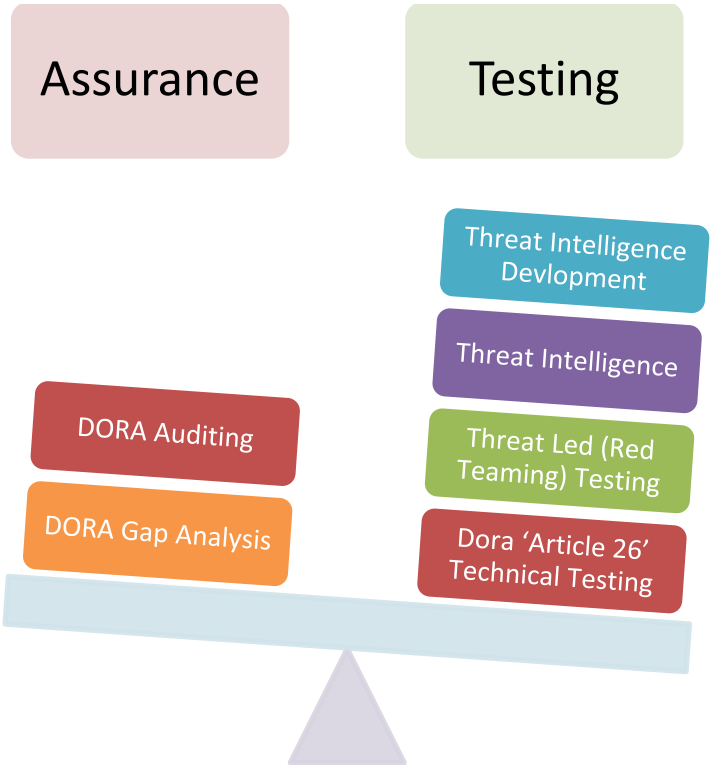
We can provide all the cyber security and information security services and resources you need to ensure your organisation follows industry-recognised best practice, enabling you to demonstrate compliance with DORA's information security risk management and testing requirements.

Chapter 27 of Article IV of DORA outlines the requirements for testing organisations to carry out Threat-Led Penetration Tests.

Below is a quick summary all of these requirements, which AMR CyberSecurity meets. As per the DORA mandate, testers should be:

- ✓ Highly capable and reputable with demonstrable expertise in threat intelligence, red teaming and penetration testing
- ✓ Capable of providing an independent audit report while protecting all sensitive data during the test
- ✓ Fully covered by relevant professional indemnity insurances
- ✓ Under strong contracts with the financial entity. The contracts must ensure complete data protection of the financial entity. It should also ensure sound management of the TLPT results
- ✓ Approved by competent authority in case of internal testers. In such cases, the threat intel provider must be external to the organisation. If a financial entity uses internal testers, they must ensure every third test is conducted by an external pentester

Outlined below are the number of services that AMR CyberSecurity has developed to specifically assist organisations with auditing, compliance, and alignment to the DORA security framework.



3.1 AMR CyberSecurity Services

AMR's services can be applied to any of an organisation's business functions, units or the whole organisation itself, and break down as:

- **DORA Gap Analysis:** As with all Gap Analysis, AMR CyberSecurity will review and analyse an organisation's current controls, processes, and procedures in relation to the defined DORA framework, cross-referencing where the organisation satisfies the minimum industry requirements and best practise or falls short of this. This allows organisations to benchmark and identify any current gaps in process and actual performance with potential or desired performance and maturity.

- **DORA Tabletop Exercises:** A DORA Tabletop Exercise evaluates your organisation's processes, tools and proficiency in relation to executive strategic and technical organisation-specific DORA-aligned scenarios.
  Each package is customisable and includes template exercise objectives, scenarios, and discussion questions as well as a collection of references and resources.
  Carefully chosen participants for the exercise are coaxed into thinking and responding like they would in an actual attack scenario.
  These exercises test the viability of an organisation's Cyber Incident Response Plans in the event of an ICT-related incident. They highlight gaps in an organisation's digital resilience posture, strengths and weaknesses. Overall, they help you refine your maturity to respond to cybersecurity and digital disruptions.
  AMR CyberSecurity also provides scenario and module questions to discuss information and intelligence sharing, as well as probing the financial organisation's processes and systems in relation to DORA.

- **Threat Intelligence Review & Scenario Development:** This service provides an opportunity to review your organisation's threat intelligence sources and collateral. By combining these sources with AMR CyberSecurity's proprietary threat intelligence analytics and extensive experience in financial sector penetration testing, we can help you develop a highly relevant and topical active threat scenario. relevant This scenario will incorporate the tools, tactics and procedures (TTP) and on host actions of recent aggressors, as well as their on-host actions, identified within the last quarter. It will be tailored to simulate real-world threats and test your organisation's ICT and data assets.

  AMR CyberSecurity will develop this threat actor profile into a fully-fledged attack "kill chain", detailing the adversary's tactics, techniques, and procedures (TTPs), as well as their actions on host. The objective is to simulate a realistic and sophisticated attack designed to exploit and compromise the organisation's:

  - Platforms
  - Systems

- Infrastructure
- Data and Information Assets

This approach ensures a thorough assessment of vulnerabilities and defences across all critical areas of your operational environment.

- **Threat Attack Simulation Scenario Execution:** AMR will execute the "threat actor" scenario developed during the first phase of the engagement. This simulation will rigorously test the organisation's security controls and monitoring systems to ensure their effectiveness in defending against attacks and mitigating the exploitation of vulnerabilities. By replicating real-world threat scenarios, this process provides actionable insights into the organisation's resilience and areas for improvement.

- **Penetration Testing:** Our certified consultants conduct a thorough technical reconnaissance of deployed assets and identify all possible aggressor entry points. They then try to 'gain access' and exploit vulnerabilities to simulate a prolonged attack and assess potential damage. Based on the test, the vulnerabilities found, their characteristics and the possible damage, AMR CyberSecurity creates a detailed report. Findings are complemented by effective remediation steps, in order to help an organisation address vulnerabilities efficiently and achieve DORA compliance.
  It's worth noting, however, that regular penetration tests also help an organisation achieve compliance with several other regulatory standards and frameworks including the GDPR, ISO 27001, PCI DSS and SOC 2, among many others. Many financial organisations already perform this testing as part of their organisational security maintenance processes.

3.2 Benefits Of DORA

DORA compliance has many benefits, including:

- **Improved cybersecurity**
  DORA requires financial institutions to implement robust cybersecurity frameworks and manage risks, which can help reduce the likelihood and impact of cyber-attacks.

- **Reduced risk of service disruptions**
  DORA requires financial institutions to implement digital risk management practices to minimise the risk of data breaches, financial losses and service disruptions.

- **Increased transparency and accountability**
  DORA requires financial institutions to share cyber threat information and report significant cyber incidents, which can help consumers understand the risks associated with their digital financial activities.

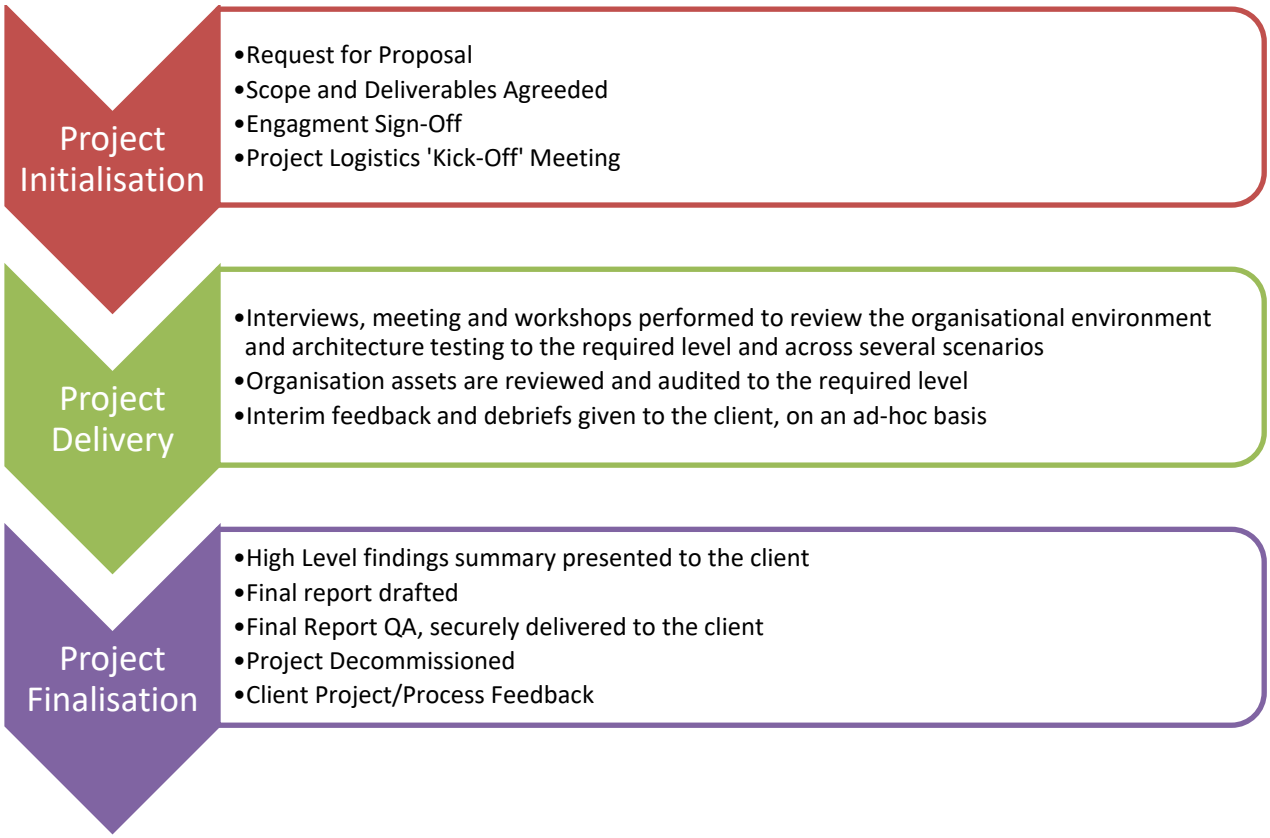
- **Streamlined operations**
  DORA can help financial institutions streamline their IT and business operations and become more agile in delivering new business solutions.

- **Improved third-party risk management**
  DORA provides rules for monitoring risks related to outsourced tasks and requires outsourcing agreements to comply with minimum contracting requirements.

4.0 Delivery Approach

AMR Cybersecurity will carry out all analysis, testing and auditing in accordance with the *AMR CyberSecurity Risk Assessment, Testing and Security Review Methodology*. This methodology has been written to align with key governmental and cyber security industry standards that have emerged to focus on key information security requirements and metrics and the following industry best practise procedures and frameworks.

Overall, at a high level the engagement process is outlined in the diagram below:



5.0 Why AMR CyberSecurity?

AMR CyberSecurity provides our customers with leading consultancy services to help them to understand and manage their risks, to achieve and maintain effective compliance regimes and to provide assurance at the project design and development stage through security architecture expertise.

AMR CyberSecurity has a highly experienced cyber security consultancy team, who hold relevant industry qualifications such as PCI DSS QSA, CISSP, CISM, CISSP, IASME Assessors and NCSC CCP and can assist you with your governance, risk, and compliance requirements.

AMR CyberSecurity can expand and highlight additional controls based on the bespoke requirements of an organisation, as well as testing, benchmarking, and auditing existing controls.

AMR CyberSecurity offers a complete all-round security posture assessment. Our highly experienced consultants have worked across many sectors including Major Corporations, Critical National Infrastructure, Banking and the Military. They understand how to communicate technical issues to both technical and non-technical audiences alike.

AMR Cyber Security has identified six key security pillars, allowing us to offer services which help organisations improve their protective and control capabilities:

- **Penetration Testing**
- **Advanced Penetration Testing**
- **Social Engineering**
- **Security Configuration Reviews**
- **Hardware and IoT Security**
- **Secure Source Code Review**

AMR CyberSecurity is a member of the leading cybersecurity bodies, including:

Assured Service Provider
in association with National Cyber Security Centre
CHECK Penetration Testing
CREST
OVS Apps
VA
PEN TEST
STAR Intelligence-led PT
THE CYBER SCHEME
OFFICIAL CYBER SCHEME SPONSOR

Our senior security consultants hold a minimum of Cyber Scheme CSTL, CREST CCT or TIGER SST (CHECK Team Leader) level qualifications and the highest level of security clearances including Security Clearance (SC) and Developed Vetting (DV).

AMR CyberSecurity is also ISO27001 and ISO9001 certified, assuring that all services that AMR offer are performed to the highest level of standards.

For more information on any of **AMR Cyber Security** Services please contact **Rachel Bi** on enquiries@amrcybersecurity.com